EMBO reports

science & society

Surveillance society

Openness is the best defence against intrusions into our private realms

David Shenk

A massive shift is taking place in the realm of privacy, and we are missing it. We have our eye on Big Brother: governments, many of them democratic, who are increasingly prying into our lives. But we are overlooking Big Dollar: corporations determined to quietly learn more and more about our habits and preferences.

Websites already silently record our every click, and e-mail services such as Google's gmail expose our messages to machine analysis. In coming years, many other consumer objects will root out and transmit our private data. The retail industry is well on its way to including tiny radiofrequency identification tags with every consumer product from underwear to milk cartons to brake pads. Such tags—consumer watchdogs call them "spy chips"—will improve shipping, stocking and shelving, and could offer new conveniences to consumers. Washing machines, for example, could recognize clothing type and make appropriate adjustments, mechanics could instantly know the age of a car part, and refrigerators could issue a warning if food has passed a spoilage date. The potential privacy incursions are also impressive. Retail stores could profile customers according to their clothing purchases and adjust in-store advertising and even pricing and credit policies. Consumers would literally be wearing their shopping tendencies on their sleeves.

These are today's tools. What about tomorrow's? The hallmarks of the new digital age are machines that are increasingly smart, small, cheap and communicative. We are, without question, headed into a world in which—mostly by our choice—the minute details of our bodies, lives and homes will be routinely tracked and shared, with the potential for more convenience and safety but also abuse. On the one hand, most of us will trade our anonymity and privacy for increased national security and cleaner, healthier and easier lives. On the other hand, we will be more vulnerable not only to malicious hackers and identity thieves but also to sophisticated marketers. This increased exposure will demand a much more nuanced definition of what privacy means, as well as specific new tools to help us navigate its components. Whether the watcher is the US National Security Agency, the phone company or the teenager next door, our increased exposure will also require new and broader vigilance.

It is not only in the virtual world where we increasingly—and voluntarily—surrender our privacy. Technologists are also aiming to creep into physical realms as yet unexamined. Paul Moskowitz, for example, would just love it if the scientists supporting his counter-terrorism squad at Brookhaven National Laboratory (NY, USA) announced that they had come up with something half as good as a dog's nose. "That is such an exquisite instrument," he said. A trained dog can reliably detect the slightest trace of a specific chemical even if the scent is masked by other pungent odours. For all the technological innovation in the twentieth century, Moskowitz said, "we don't have anything that can touch that yet."

We are sitting in his office, 70 miles from New York City, discussing the recently restored Grand Central Terminal in midtown Manhattan. As far as counterterrorism experts are concerned, Grand Central might as well have a giant red bull's-eye painted on the floor: the station seems that good a target for the next large terrorist attack. This is what scientists and technologists such as Moskowitz have become obsessed with since the morning of September 11, 2001. Where is the next intended ground zero? And what can be done to protect it?

> We are, without question, headed into a world in which—mostly by our choice—the minute details of our bodies, lives and homes will be routinely tracked and shared…

Police, of course, have surveillance cameras trained on the 700,000 commuters passing through Grand Central each day, along with assorted other hi- and low-tech detectors looking for conventional explosives, nuclear and dirty bombs, chemical weapons and bioweapons. Hundreds of human detectives, both uniformed and plain-clothed, also keep a close eye on things. But nothing in their assorted surveillance tool belt comes close, Moskowitz said, to the slightly moist olfactory surveillance machine developed in the Canidae family during four billion years of evolution. A single dog's nose could someday save Grand Central Terminal from collapse.

Against that furry gold standard, scientists are trying to speed up the process of discovery. In the post-9/11 landscape, we need dog-nose equivalents for facial recognition and to detect money laundering, encrypted e-mail, bioweapons and suitcase bombs—and we need them now. It seems that our intelligence agents cannot adequately detect or track terrorists living in the USA; that we cannot effectively screen ships or trucks for nuclear weapons; and that even with a sky full of spy satellites, the search for the world's most wanted man, Osama bin Laden, has still turned up nothing.

> Whether the watcher is the US National Security Agency, the phone company or the teenager next door, our increased exposure will also require new and broader vigilance

We are hurtling towards constant electronic scrutiny—of the enemy and of ourselves. Increasingly, our world is full of ID checks, surveillance cameras, body scans, fingerprint databases, e-mail sifters and mobile-phone interceptors designed to ensure that electronic trails do not grow cold. Add to that mundane domestic gadgets such as nanny-cams, wireless heart monitors, swipe-in school and workplace IDs, and E-ZPass—a tag that attaches to your car windshield and electronically deducts highway tolls from your prepaid account—and you begin to get some idea of this ever-examined, ever-watched landscape of total surveillance.

Late one autumn day at the aquatic centre in Ancenis, France, something went quietly, horribly wrong. With its two well-kept pools and teaching facilities, the centre serves as a modern swimming hole for an entire sector of historic Brittany, attracting 150,000 French villagers a year. An 18-year-old named Jean-François LeRoy was a regular, coming often in the early evenings to swim laps in the 25-metre pool.

Drownings are often difficult to spot; they are rarely the splashy, flailing events depicted on television. Most are near-silent episodes in which the victim sinks quickly out of view. On this particular day maybe the lifeguards were not paying as close attention as they should have been. Certainly they believed the trim, athletic LeRoy was not a high-risk swimmer. But on this evening LeRoy was practicing apnoea swimming—testing how far he could swim underwater on one breath—and at some point, without making any visible or audible disturbance on the water's surface, he blacked out. The guards failed to notice as he stopped swimming and descended to the bottom of the pool. It would take him as little as four minutes to die.

Although the human lifeguards watching the pool were oblivious, 12 large machine eyes deep underwater were seeing everything. Just nine months earlier the centre had installed a state-of-the-art electronic surveillance system called Poseidon (Vision IQ; Boulogne, France)—a network of cameras that feeds a computer programmed to distinguish between normal and distressed swimming. Poseidon covers a pool's entire swimming area and can distinguish among blurry reflections, shadows and actual swimmers. It can also tell when real swimmers are moving in a way they are not supposed to. When the computer detects a possible problem, it instantly activates a beeper to alert lifeguards and displays the exact incident location on a monitor.

Sixteen seconds after Poseidon noticed the large, sinking lump that was LeRoy, lifeguards had him out of the pool and were initiating cardiopulmonary resuscitation. He started breathing again. After one night in the local hospital, he was released with no permanent damage. Poseidon—and, more precisely, the French mathematicians who devised it—had saved LeRoy's life. Machines such as Poseidon will redefine how we live. Think of your life before the answering machine, the automated teller machine, or e-mail. Think of your grandparents' lives before the television or the airplane. Think of your great-grandparents' lives before the telephone.

Machines will recognize our faces and our fingerprints. They will watch out for swimmers in distress, for radioactivity-laden and germ-carrying terrorists, for drivers speeding and running red lights, for diabetics and heart patients. Imagine devices that monitor the breathing rhythms of infants as they sleep, watch toddlers at day care and track children as they go to and from school. Machines might watch our calorie intake and energy output, monitor air quality in our homes, and look out for mice and bugs.

> As time and technology march on, less and less will escape the attention of sophisticated machines

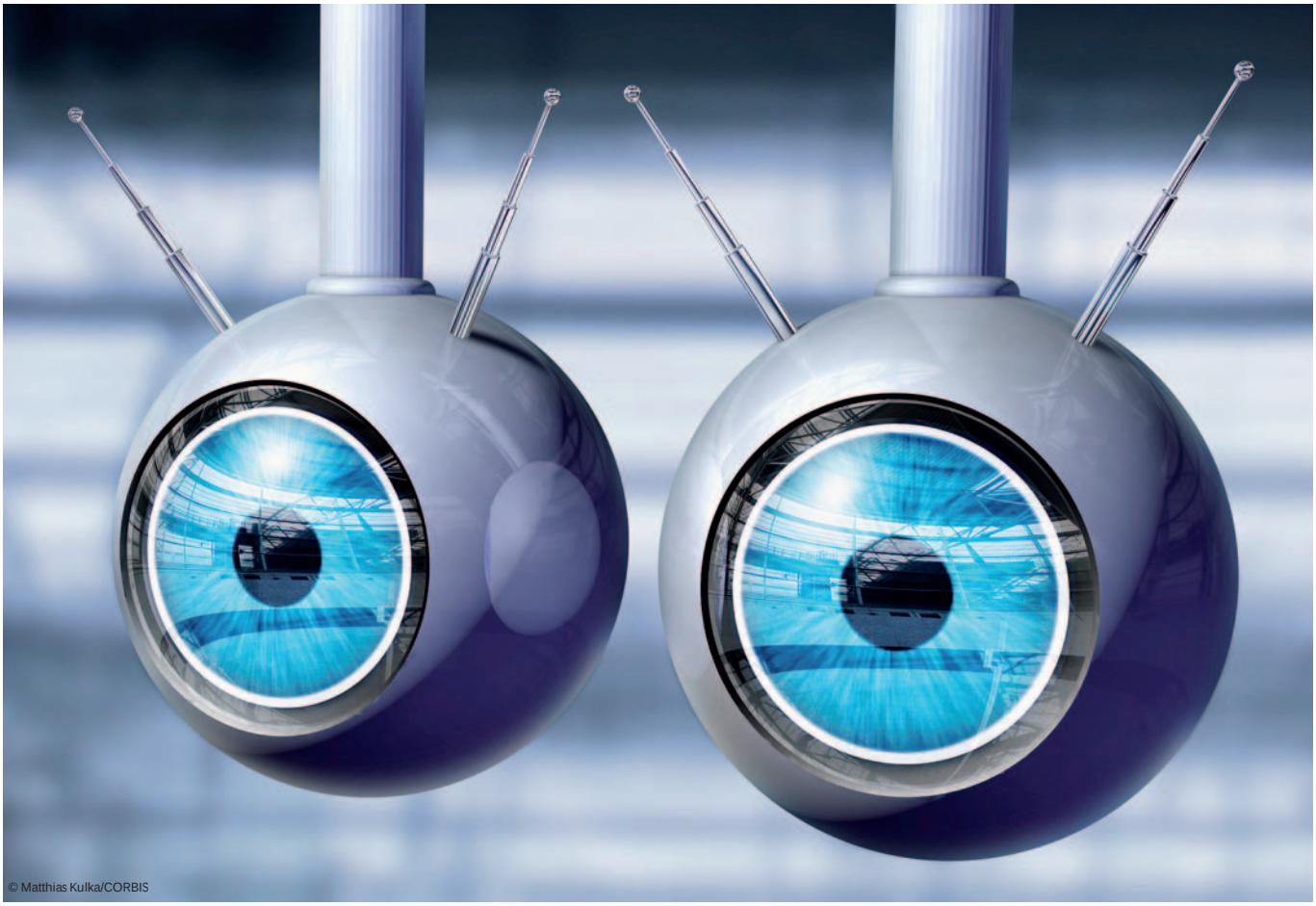
Envision sensors as large as walls and as small as molecules in your bloodstream, sending quiet signals to nearby computers, which will process and relay information to you, your doctor, your lawyer, your grocer, your building manager, your car mechanic, your local fire or police department. As time and technology march on, less and less will escape the attention of sophisticated machines. These digital eyes, ears and noses, we hope, will also protect our cities from cataclysm. But as Moskowitz and others make abundantly clear, we are not there yet.

On September 10, 2002, as the USA braced itself for the first anniversary of the 9/11 attacks, a 708-foot container ship named *Palermo Senator* slowly motored towards the East Coast from the Mediterranean to unload hundreds of 40-foot containers. Every day, 19,000 such containers arrive in the USA. A nuclear device hidden in just one of them could kill millions of people and cripple any port city. By virtue of the sheer volume of shipments, seaports are considered perhaps the most vulnerable entry point for weapons of mass destruction.

On this ominous day, authorities had a tip that an approaching vessel might be carrying such a weapon. They boarded a handful of ships identified as high risk. After a rigorous onboard inspection of Palermo Senator, someone detected radiation emanating from the ship. Officials immediately ordered the vessel to a safer distance of six miles offshore, where Coast Guard, Federal Bureau of Investigation (FBI) and Department of Energy specialists along with a team of Navy SEALs spent two days combing the boat for the radiation source. They finally pinpointed a large shipment of ceramic tiles. The radiation was natural and safe. False alarm.

> …what Orwell did not prophesy in his novel *Nineteen Eighty-four* was just how pervasive surveillance would be in free societies…

But the incident was profoundly worrisome as a demonstration of how costly and cumbersome it is to detect a nuclear needle in the shipyard haystack. And a false alarm still commands resources. Since 9/11, similar false alarm dramas play themselves out on a smaller scale many times every day: the air traveller whose name happens to be the same as one on a terrorist watch list; the X-ray machine or metal detector that seems obsessed with a car key. Many New York City police officers now sport low-cost radiation detectors sensitive enough to pick up small amounts of radiation but crude enough to be set off by harmless medical equipment—or even recently irradiated cancer patients. "False positives can create an unmanageable backlog and can also lead to what we call organizational fatigue,"



said Moskowitz. "People get worn out and become far less alert." The singular goal of any surveillance system, then, is to ferret out serious threats effectively while keeping false positives down to a negligible level.

One creative challenge is to integrate extraordinary new surveillance tools into ordinary infrastructure. Detectors might be effectively attached to cranes or built into highway exits. "We even thought of attaching large gamma-ray detectors to the underside of the Verrazano-Narrows Bridge [in New York City] to scrutinize ships passing beneath it," explained Peter Vanier from Brookhaven's Nonproliferation and National Security Department. Or detectors might be attached to helicopters or to pilot boats to examine ships before they enter the harbour.

It might not be the kind that sees gamma rays, but a surveillance tool could one day reside in every pocket. Various European and Asian countries are introducing a citizen smart card that would act as an official national ID. It could hold personal medical history, social security information, and serve as a passport, train pass, toll card, credit and debit card, long-distance phone card and library card. Such a card could tap into systems that talk to each other, merging the worlds of consumer convenience and citizen surveillance. Your e-mail will know your mobile phone, which will know your shopping list, which will know your online pharmacy, which will know your courier-service account—all of it potentially available to marketers or hackers and just one search warrant away from government inspection. The US Treasury Department's Financial Crimes Enforcement Network already brings together financial, law enforcement and commercial databases and a considerable array of government agencies in a vast attempt to ferret out money laundering and other financial crimes. A new suite of commercial software tools called COPLINK, designed on the basis of research from the Artificial Intelligence Lab at the University of Arizona (Tucson, AZ, USA), uses artificial-intelligence algorithms to search the Internet and confidential crime databases, helping law enforcement agencies to connect all the dots in a complex investigation.

In totalitarian regimes that do not recognize citizens' rights to privacy, this sort of all-seeing, all-knowing surveillance obviously threatens to become the terrifying realization of George Orwell's Big Brother. But what Orwell did not prophesy in his novel *Nineteen Eighty-four* was just how pervasive surveillance would be in free societies, introduced not by despots but in the name of liberty, safety and security.

Take Great Britain, Orwell's native land. In the 1970s and '80s, municipalities tentatively began installing closed-circuit television (CCTV) cameras on streets and in parks, transit stations, stadiums and shopping areas. Then, in the 1990s, attacks by the Irish Republican Army and a threatening rise in urban crime prompted a massive proliferation of CCTVs. In the ensuing decade, so many cameras were installed that the government lost count.

With more than four million CCTV cameras nationwide, the deployment certainly amounts to more than anywhere else in the world, somewhere around one for every 15 people. The average visitor to London, estimates British sociologist Clive Norris, is now captured on video 300 times in a single day. In an exhaustive study of surveillance trends in the UK, Norris and his colleague Michael McCahill concluded that cameras are becoming so omnipresent that all Britons should assume their behaviour outside the home is monitored (Norris & McCahill, 2003; Norris, 2002).

The actual effectiveness of the cameras is far from clear. The most rigorous studies show a sustained and dramatic reductive effect in some areas, according to McCahill and Norris, and a negligible impact in others. Nevertheless, the public seems to approve of the cameras. Buoyed by that support, the British government is now moving ahead to the next phase: an ambitious vehicle-surveillance system designed "to reduce serious and volume crime by denying criminals the use of the roads" (Bath & North East Somerset Council, 2003).

> In a city and a world that suddenly feels much less safe, being watched has its discomforts, its reassurances, even its thrills

Relying on optical character-recognition software and criminal databases, fixed and mobile cameras available to every police force in England and Wales will scan license plates and flag suspicious ones. Public surveillance in Britain, suggests urbanist Stephen Graham, has emerged as a fifth utility, joining water, gas, electricity and telephones as an essential public service (Graham, 2002).

Public video systems are now proliferating in Melbourne, Sydney, Vienna, Berlin, Brussels, Dublin, Baltimore, Palm Springs and scores of other cities small and large. In Jerusalem, Israeli officials have packed the tangled alleys of the Old City with surveillance cameras. In Paris, ubiquitous road cameras help to regulate traffic, and some 2,000 cameras on city buses detect and deter crime. Police in Monaco have so saturated their streets with cameras as to make them confident that virtually all future street crime will be recorded. So only a handful of years after the end of the Cold War, which was largely a battle between intrusive regimes and open, democratic regimes, the democratic winners are now adopting their own brand of public intrusiveness for the sake of comfort and security.

The lack of protest or genuine public debate is unnerving to privacy advocates. "The cameras are not just coming, they're here now," warns New York civil-rights lawyer Norman Siegel. "There has been an explosion of video surveillance in public spaces without any real public debate about the pros and cons. That's remarkable. You'd think there would be a referendum somewhere."

The USA is moving decidedly in the same direction as is Britain. A showcase for some of what could be in store presented itself at the 2002 Winter Olympics in Salt Lake City, Utah. On the heels of 9/11, the Games represented a potential terrorist target. Quietly nestled among the tens of thousands of athletes, dignitaries and tourists was a team of agents from the FBI, Federal Aviation Authority, US Secret Service, State Department, Utah National Guard and other federal, state and local agencies. Together they ran an unprecedented security operation that transformed the area into a veritable fishbowl.

At the heart of the operation was a digital video system that processes input from many cameras, archives everything for future review, screens for pre-programmed problem signs such as suspicious movement or light changes, and distributes customized portions of the video stream to any authorized computers on the system. At any time during the 17-day games, video images from inside and outside sports venues, from all around Salt Lake City's Olympic Square and from key angles surrounding important parts of the city infrastructure could be watched simultaneously at the Olympic Coordination Center, at FBI headquarters in Washington, DC, and, if need be, in the White House Situation Room.

On the morning of the opening day, Secret Service Director Brian Stafford was asked in an interview how visible security would be in the Olympic stadium that night. Stafford replied: "You'll see some countersnipers, you may see some counterassault teams. There's a lot more you won't see" (Stafford, 2002).

> Openness is inherently democratic, and such disclosures allow consumers to react as they wish

With deterrence such an important objective of the surveillance, Stafford and other security officials in Salt Lake City were only too happy to emphasize that most of the watching was invisible. Then US Attorney General John Ashcroft, after his pre-games tour of Olympic security, declared: "What's happening here has never happened before. This will set a new standard" (Gorov, 2002).

Did Salt Lake City also set a new *social* standard? Extraordinary concern after 9/11 called for extraordinary measures at the 2002 Games, and there was no outcry from the public at large or from privacy advocates. But will the welcoming attitude towards heightened surveillance at the Olympics transfer to attitudes about more ordinary, public places?

Signs point to yes. In the coastal resort town of Virginia Beach (VA, USA), police have installed a facial-recognition system that looks for people connected to outstanding arrest warrants. In Washington, DC, the National Park Service is installing surveillance cameras around federal monuments. And in the same city, Woodrow Wilson High School has replaced morning roll call with an electronic ID-recognition system that not only keeps tabs on everything from class attendance to outstanding library fees, but also reminds people that the surveillance is personal by playing a special jingle for every birthday boy and girl.

Meanwhile, back in New York City, a trendy new Bowery bar located roughly between ground zero and Grand Central Terminal has inaugurated a kind of surveillance chic. The Remote Lounge is packed with video cameras and monitors, and the entrance features a brightly lit disclaimer: "Upon entering these premises your name, image, voice, and likeness may be broadcast live over the Internet.... You hereby agree that you have no expectation of privacy for any acts or statements made on these premises."

It is half legal waiver, half social dare. Inside, patrons toggle constantly between camera angles, spying on—and being spied on by—everyone else. In a city and a world that suddenly feels much less safe, being watched has its discomforts, its reassurances, even its thrills. Clearly for the moment—for better or worse—surveillance surrounds us and shapes us.

The good news is that there is a simple and elegant standard for all surveillance minders to adopt: citizens have the right to

know—in real time—when and how they are being monitored. Just as some US states require "all party consent" for telephone recordings, so it should be with e-mail, web surfing, walks in the park or any activity being captured by a distant unseen party. Such disclosures might look like "Welcome to Shop-Mart. Your shoe size is 9," or "All persons entering City Park are subject to video and audio surveillance by the Metropolitan Police Department," or "Thank you for browsing at BooksOnLine where page views are recorded and attached to your file. Click here if you prefer to browse anonymously." Openness is inherently democratic, and such disclosures allow consumers to react as they wish. And if the snooping is too embarrassing for companies or public officials to acknowledge, their noses should not be there to begin with.

ACKNOWLEDGEMENTS

This text is a modified version of an article originally published in *National Geographic Magazine* in November 2003. With kind permission from the National Geographic Society, Washington, DC, USA.

REFERENCES

Bath & North East Somerset Council (2003) CCTV—Automatic Number Plate Recognition System. www.bathnes.gov.uk

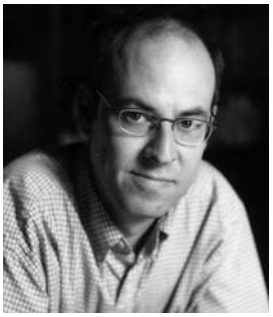
Gorov L (2002) Salt Lake sets massive security for Olympics. *The Boston Globe*, 20 Jan

Graham S (2002) CCTV: The stealthy emergence of a fifth utility? *Planning, Theory & Practice* **3:** 237–241

Norris C (2002) From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. In Lyon D (ed) *Surveillance As Social Sorting: Privacy, Risk and Automated Discrimination* pp 249–281. London, UK: Routledge

Norris C, McCahill M (2003) Victims of surveillance. In Davies P, Jupp V, Francis P (eds) *Victimisation: Theory, Research and Policy*. London, UK: Macmillan

Stafford B (2002) Today Show. *NBC TV*, 8 Feb



David Shenk, author of *Data Smog* and *The End of Patience*, among other books, lives in New York City, NY, USA. He writes and lectures often about the unintended consequences of technology. www.davidshenk.com. E-mail: dshenk@yahoo.com

doi:10.1038/sj.embor.7400735